AO 106 (Rev. 7/87) Affidavit for Search Warrant

United States District Court

DISTRICT OF DELAWARE

In the Matter of the Search of

(Name, address or brief description of person, property or premises to be searched)

[redacted] Rehoboth Beach, Delaware, described more particularly on Attachment 1

REDACTED

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

CASE NUMBER: 04-44M-LPS

FILED
2004 APR 29 PM 2:57
CLERK U.S. DISTRICT COURT
DISTRICT OF DELAWARE

I Special Agent Walter J. Steffens, Jr. being duly sworn depose and say:

I am a(n) Federal Bureau of Investigation Special Agent and have reason to believe
Official Title

that ☐ on the person of or ☒ on the property or premises known as (name, description and/or location)

[redacted] Rehoboth Beach, Delaware, described more particularly on Attachment 1

in the _____ District of Delaware

there is now concealed a certain person or property, namely (describe the person or property to be seized)

items described on Attachment A

which is (state one or more bases for search and seizure set forth under Rule 41(b) of the Federal Rules of Criminal Procedure)

evidence of a crime

concerning a violation of Title 17 United States code, Section(s) 506(a) & 18 USC 371 & 2319.

The facts to support a finding of Probable Cause are as follows:

Affidavit attached

FILED
JAN 25 2006
U.S. DISTRICT COURT
DISTRICT OF DELAWARE

Continued on the attached sheet and made a part hereof. ☒ Yes ☐ No

Signature of Affiant
Walter J. Steffens, Jr.
Special Agent, FBI

Sworn to before me, and subscribed in my presence

April 29, 2004 at Wilmington, Delaware
Date City and State

Honorable Mary Pat Thynge
United States Magistrate Judge

Attachment 1

[redacted] in Rehoboth Beach, Delaware. [redacted] is a taupe bungalow with white trim and black shutters. The front door is black with a brass kick plate. A garage (taupe with a white door) is attached to the house. A mailbox is mounted on a white post set at the curb in front of the house. The numbers [redacted] are mounted vertically on the mailbox post.

Attachment A: Items to be seized

Items evidencing violations of Title 17, United States Code, Section 506(a), and Title 18, United States Code, Sections 371 and 2319(a), including but not limited to the following:

1. Computer files protected by copyright, including but not limited to software, game, movie and music titles.

2. Computer log files relating to copyright infringement, including but not limited to transfer logs of FTP uploads and downloads.

3. Computer files containing communications between individuals relating to copyright infringement, including but not limited to IRC and instant messaging logs, and emails.

4. Programs or software used by those engaging in copyright infringement, such as burning tool programs and software used for FTP file transfers (e.g. FlashFXP).

5. Records, in whatever form, of user names and passwords to "warez" sites and secure communication services.

6. Computer hardware, meaning any and all computer equipment. Included within the definition of computer hardware is any electronic device capable of data processing (such as central processing units, laptop or notebook computers, personal digital assistants, and wireless communication devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media); related communications devices (such as modems, cables and connections); storage media, defined below; and security devices, also defined below.

7. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

8. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

9. Data security devices, meaning any devices, programs, or data -- whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, but are not limited to, user names and passwords; data security hardware (such as encryption devices, chips, and circuit boards); data security software or information (such as test keys and encryption codes); and similar information

that is required to access computer programs or data or to otherwise render programs or data into usable form.

10. Records, in whatever form, referencing or regarding warez activity, warez sites, or individuals who participate in warez activity.

11. Storage media capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and backing up electronic data used to conduct warez activity or which contains material or data obtained through warez activity. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment, such as fixed hard disks, external hard disks, removable hard disks, floppy diskettes, compact disks (CDs), digital video disks (DVDs), tapes, optical storage devices, laser disks, or other memory storage devices.

12. Records, in whatever form, of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes, books, diaries, and reference materials.

13. Records, in whatever form, pertaining to accounts held with Internet Service Providers or of Internet use.

14. Evidence or records, in whatever form, relating to the ownership, occupancy, or use of the premises to be searched.

AFFIDAVIT

I, Walter J. Steffens, Jr., being duly sworn, hereby depose and state as follows:

Introduction

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed for approximately twenty years. I was assigned to the FBI office in Omaha, Nebraska from 1984 to 1988. I was assigned to the FBI office in Boston, Massachusetts, from 1988 to 1997. Since 1997, I have been assigned to the FBI Resident Agency in Dover, Delaware. I have been the affiant for a number of investigations, including three "roving" Title III investigations, one wire Title III investigation, and numerous affidavits in support of applications for search warrants and arrest warrants.

2. My experience as a FBI agent has included the investigation of cases involving the use of computers and the Internet to commit violations of fraud, child pornography, intrusion and intellectual property laws. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, and various other criminal laws and procedures. I have participated in the execution of several search warrants involving the search and seizure of computer equipment.

3. I make this affidavit in support of an application by the United States of America for the issuance of a warrant to search the premises described below ("the premises") for the items described in Attachment A, which constitute evidence, contraband, fruits, or instrumentalities of violations of the criminal conspiracy and copyright laws, namely Title 17, United States Code, Section 506(a), and Title 18, United States Code, Sections 371 and 2319. Title 17, United States Code, Section 506 provides, in pertinent part:

> **(a) Criminal Infringement.** Any person who infringes a copyright willfully . . . (2) by the reproduction or distribution, including by electronic means,

> during any 180-day period, of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000 [shall be punished as provided under Section 2319 of Title 18, United States Code].
>
> **(b) Forfeiture and Destruction.** When any person is convicted of any violation of subsection (a), the court, in its judgment of conviction shall, in addition to the penalty therein prescribed, order the forfeiture and destruction or other disposition of all infringing copies or phonorecords and all implements, devices, or equipment used in the manufacture of such infringing copies or phonorecords.

Title 18, United States Code, Section 2319(c) states, in pertinent part, that any person who violates 17 U.S.C. § 506(a)(2):

> (1) shall be imprisoned not more than 3 years, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 10 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of $2,500 or more;
>
> . . . .
>
> (3) shall be imprisoned not more than 1 year, or fined in the amount set forth in this title, or both, if the offense consists of the reproduction or distribution of 1 or more copies or phonorecords of 1 or more copyrighted works, which have a total retail value of more than $1,000.

4. The facts set forth in this affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of a cooperating witness, as related to me by other law enforcement officers; my review of documents and computer records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

5. This application is being made to further an investigation of organized criminal groups that use computers and the Internet to engage in large-scale violations of federal criminal copyright laws. Through experience gained from participation in this investigation, I have become familiar with the manner in which these organized groups of individuals – also known as "warez groups" – engage in the illegal reproduction and distribution of copyrighted works over the Internet.

6. Evidence collected during this investigation has established that an individual utilizing the online nickname "cinema" is a member of the warez scene in general as well as a member of at least one specific, identified warez group. The evidence summarized below supports a finding of probable cause that "cinema," individually and in conspiracy with others, has caused the illegal reproduction and distribution of more than 10 copies of copyright-protected software worth more than $2,500 during a 180-day period, and that he did so using a computer system or systems and electronic media located at the premises to be searched.

Summary of Relevant Computer and Internet Concepts

7. **"Warez"** and **"pirated computer software"** are terms used to describe copyright-protected computer software that is distributed over the Internet in violation of copyright law.

8. **"Warez group"** refers to an organized group of individuals who engage in the unauthorized and illegal reproduction, modification and distribution of copyrighted computer software, games, and movies on the Internet in violation of federal criminal copyright law. Collectively, these groups and other individuals comprise what is called the **"warez scene"** -- a subculture of the Internet dedicated to the illegal piracy of copyrighted software, games, movies, and music. In the past three years, more than fifty individual members of identified warez groups have been convicted of criminal copyright violations in the United States.

9. **Internet Protocol Address ("IP address"):** An Internet Protocol (IP) Address is a unique numeric address used to identify computers on the Internet. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic sent from and directed to that computer is directed properly from its source to its destination. IP addresses are typically assigned by Internet service providers ("ISPs"), such as AOL, Earthlink or cable companies. An ISP might assign a different IP address to a customer each time the customer makes an internet connection (so-called "dynamic IP addressing"), or it might assign an IP address to a customer permanently or for a fixed period of time (so-called "static IP addressing"). Either way, the IP Address used by a computer attached to the Internet must be unique for the duration of a particular session; that is, from connection to disconnection. ISPs typically log their customers' connection, which means the ISP can identify which of their customers was assigned a specific IP address during a particular session.

10. **Domain Names:** Numerical IP addresses may have corresponding domain names. For instance, the IP address "149.101.10.40" resolves to the corresponding domain name "www.cybercrime.gov." The Domain Name System ("DNS") is an Internet service that associates each domain name with an IP address. This mapping function is performed by DNS servers located throughout the Internet. DNS allows a user knowing only a domain name to reach a computer without having to know its IP address. In general, a registered domain name should resolve to a numerical IP address.

11. **File Transfer Protocol ("FTP")** is a communication protocol for transferring files between computers connected to the Internet.

12. The terms **FTP site** and **FTP server** generally refer to computers connected to the Internet that serve as large storage databases for software or other digital files. Users can transfer, upload or download, software and other files through the FTP protocol. In the warez scene, FTP sites are most often used to store, distribute and trade illegal warez. These sites are not accessible to the general public. Access to warez FTP sites is typically controlled through a variety of security mechanisms. For example, a user is typically required to log onto an FTP site using a screen name and password approved by one of the site's system administrators. In most cases, the final level of authentication, which is done automatically, requires the user to attempt access to the server only from a specific IP address previously supplied to the administrator(s). Failure to meet any of the security requirements results in the denial of access to the FTP server.

13. **Log files** are computer-generated files containing information regarding the activities of computer users, processes running on a computer, and the activity of computer resources. FTP servers can generate **transfer logs** that capture information about each FTP file transfer. Transfer logs may include the date of transfer, name of the file transferred, direction of transfer (upload or download), the name or nickname of the individual accessing the computer, and the IP address of the computer sending or receiving the file.

Background of the Warez Scene

14. In the early 1990s, teams of computer hackers organized themselves into various international groups that became an underground Internet society known as the "warez scene." The leading warez groups compete against each other to attain the reputation as the fastest provider of high-quality pirated computer software, including utility and application software, console games,

and movies. These warez groups specialize in being the first to release new pirated software to the warez community for unauthorized reproduction and distribution worldwide.

15. Preparing new pirated software for release and distribution to the warez scene generally requires a number of different steps. First, an individual known as a "supplier" will post an original digital copy of new computer software to the Internet "drop site" of a particular warez group. Frequently, "suppliers" are company insiders or software testers who can provide final versions of new product before it is released to the public. Once the new supply is posted to the "drop," another individual, known as a "cracker," retrieves the software and removes or otherwise circumvents its copyright protection controls, including serial numbers, tags, duplication controls, and/or security locks. Once successfully cracked, the software is tested and packed for final posting to the "drop" site, where it is picked up by couriers for rapid distribution to other warez sites worldwide. The entire process can occur within a matter of hours.

16. Active participants in the release and distribution process are rewarded in a variety of ways, often with privileged access to large, non-public caches of pirated works on warez FTP sites. With this access, a user is able to download vast amounts of pirated software for personal use or further distribution.

17. Members of the warez scene often use "real time" software applications to communicate with each other online. These methods of communication include Instant Messenger ("IM"), password-only Internet relay chat ("IRC"), and ICQ (literally, "I seek you"). These communication sessions can be logged and therefore preserved by any of the participants.

Summary of Investigation

18. A cooperating witness ("CW") assisted in this investigation. CW was previously a member of the Warez scene, and has entered into a cooperation agreement with the government pursuant to which CW will receive consideration in return for his assistance. CW has been assisting in an undercover investigation for at least five months. CW's online activities and communications are logged, with CW's consent, by monitoring software. In addition, the information provided by CW has been extensively corroborated by independent investigation. The agents supervising CW believe CW to be truthful and reliable.

19. Because of CW's status as a trusted member of the warez scene, CW has access to FTP servers used to store and distribute warez. CW, or investigators working with him/her, are able to obtain from these servers the directory listings of all of the digital files that are available for downloading by those given authorized access to the server. In some cases, CW's level of access also allows him/her, or investigators working with CW, to obtain the FTP transfer logs which record, among other things, the IP address of any user who supplies a file to, or obtains a file from, the server, as well as the date, time, file name, file size and direction (upload or download) of each file transfer. This same level of access allows CW and investigators to view and copy the user list(s) and authentication information for all authorized users of the computer.

Transfer Log Analysis

20. An examination of the transfer logs from a warez FTP server for the time period of November 3, 2003, through March 29, 2004, indicates that an individual utilizing the online nickname "cinema" downloaded approximately 94 software titles from the FTP server during that time period. Those titles include movies (Lord of the Rings: The Return of the King, The Last

Samurai), PC and console games (The Simpsons Hit and Run, Star Wars Knights of the Old Republic) and utility software (Adobe Photoshop CS V8.0, Norton Systemworks Pro 2004).

21. The log files for the same server also captured the IP address assigned to the computer from which "cinema" caused files to be uploaded or downloaded when transferring software, games and movies from or to the FTP server. Specifically, on January 5, 2004, "cinema" accessed the warez FTP server and initiated a file download from a computer assigned the IP address [redacted] This IP address is registered to the ISP Verizon.

22. On or about January 15, 2004, and March 9, 2004, subpoenas were served on Verizon requesting subscriber and related account records for the subscriber assigned the IP address [redacted] for the aforementioned relevant time period. In response to each subpoena, Verizon provided records indicating that IP address [redacted] was assigned to Verizon subscriber Jeff Balk, residing at [redacted] Rehoboth Beach, Delaware, during the aforementioned relevant time period.

23. On April 14, 2004, I determined that on April 12, 2004 Jeff Balk, d.b.a. EXP GAYZETTE, J&J Publishing, former address [redacted] Rehoboth Beach, Delaware, had filed a change of trade name and change of location with the City of Rehoboth Beach, Delaware. The changes were noted on the application for a business license filed at the Business License Office for the City of Rehoboth Beach (DE). The trade name was changed from EXP GAYZETTE [sic] to EXP MAGAZINE. The trade location was changed from [redacted] Rehoboth Beach, Delaware, to [redacted] Rehoboth Beach, Delaware. The application listed Jeffrey Balk, [redacted] as one of the officers of the corporation. (19971 is the zip code for Rehoboth Beach, Delaware.) Missouri was listed as the state of incorporation.

24. On or about March 23, 2004, through March 29, 2004, transfer logs obtained from the warez FTP server indicate that "cinema" initiated the transfer of 7 movies (from one FTP site to another FTP site) by using a computer assigned IP address [redacted] This IP address is registered to Comcast IP Services (Comcast).

25. On or about April 13, 2004, a subpoena was served on Comcast requesting subscriber and related account records for the subscriber assigned the IP address [redacted] In response to the subpoena, Comcast provided records indicating that IP address [redacted] was assigned to Comcast subscriber Jeff Balk, residing at [redacted] Rehoboth Beach, Delaware. Your affiant is aware that residential cable modem service is accessible only at that residence.

26. Documents provided to investigators by CW indicate that "cinema," who CW does not know by real name, is a member of the warez community and a member of a specific warez group known as "ESOTERiC."

27. Warez groups operating an FTP site generally take steps to ensure the quality of their software, games or movies available on the site. Warez which do not function properly are not uploaded to the site, and if an uploaded warez title is found to be defective, it is removed from the site (a deletion process known as "nuking"). As of March 28, 2004, the aforementioned FTP server accessed by "cinema" contained approximately 1233 titles of business software, games and movies. A directory listing of software titles from this FTP server was provided to the Business Software Alliance (BSA). The BSA represents various software companies involved in the development and manufacture of business utility and application software. A BSA analysis of the FTP title directory confirmed that the FTP directory list included software products owned by BSA clients which were subject to copyright protection and collectively exceeded $80,000 in retail value.

Other Information

28. I personally viewed the premises to be searched: [redacted] is in a small development of newly constructed homes, [redacted] Rehoboth Beach, Delaware. [redacted] s a taupe bungalow with white trim and black shutters. The front door is black with a brass kick plate. A garage (taupe with a white door) is attached to the house. A mailbox is mounted on a white post set at the curb in front of the house. The number[redacted]re mounted vertically on the mailbox post.

29. Delaware Department of Motor Vehicle information for Jeffrey M. Balk, Delaware driver's license[redacted] lists an address of [redacted] This information was posted on January 22, 2003, when Balk surrendered his Missouri driver's license, number[redacted] It has not been updated to reflect Balk's current address of[redacted] [redacted]which is listed on the Rehoboth Beach business license described in paragraph 23, above, and in the information describing IP address[redacted] provided by Comcast (para 25, above).

30. Deljis records reflect that Jeffrey M. Balk is[redacted]

Evidence, Contraband, Fruits, and Instrumentalities of the Crime

31. Based on my experience and information that I have obtained from others experienced in such investigations, I have learned that warez scene members typically maintain at their residence or place of business various pieces of computer hardware; computer software; computer storage media; computer records; paper and electronic notes regarding software piracy; and paper and electronic correspondence with others who engage in software piracy, within the meaning of Title 17, United States Code, Section 506(a), and Title 18, United States Code, Section 2319. All

of these items constitute evidence, contraband, fruits, or instrumentalities of violations of Title 17, United States Code, Section 506(a), and Title 18, United States Code, Sections 371 and 2319.

32. I have also learned that individuals who participate in copyright infringement through the warez scene often transfer or copy their illegally obtained computer software, games, and movies to computer storage media and other electronic systems that are not connected to the Internet. This is usually done to facilitate ease of use. Whether stored on a computer system connected to the Internet or on any other type of computer storage media, such illegally obtained computer software, games, and movies are routinely kept and collected by warez participants for many months or even years. This is often done because the warez participant wants to be able to reinstall the software or media whenever convenient, or because he or she wants to use those titles to trade for other software and media. In addition, I have learned that, even if illegally obtained software is later deleted by a warez participant, the computer system that was previously used to store that software often retains evidence of the offense. This is because files deleted by the user may still remain (in whole or in part) on the storage media, as deletion of a file may not remove that data completely from the media.

33. Additionally, the aforementioned facts provide evidence of probable cause to believe that Jeffrey M. Balk, utilizing the online nickname "cinema," maintains computer(s) at his residence, [redacted] Rehoboth Beach, Delaware, which have been used to commit the offense of criminal copyright infringement; that is, to cause the unauthorized reproduction and distribution by electronic means during a 180-day period of one or more copies of copyrighted software having a total retail value exceeding $2,500. Therefore, the computer hardware, software, passwords, data security devices, and computer data described in Attachment A constitute not only evidence, contraband, fruits, and instrumentalities of these offenses, but also constitute "implements, devices,

or equipment used in the manufacture of" infringing copies of copyrighted works, and are thereby subject to criminal forfeiture and destruction or other disposition pursuant to 17 U.S.C. § 506(b).

34. Based upon my knowledge, training, and experience, as well as information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices. I also know that during the search of the premises it is rarely possible to complete on-site examination of computer equipment and storage devices for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is rarely possible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

b. The best practices for analysis of computer systems and storage media rely on rigorous procedures designed to maintain the integrity of the evidence and to recover "hidden," mislabeled, deceptively-named, erased, compressed, encrypted, or password-protected data while reducing the likelihood of inadvertent or intentional loss or modification of data. A controlled environment, such as a law enforcement laboratory, is typically required to conduct such an analysis properly.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. The hard drives commonly included in mere desktop computers are

capable of storing millions of pages of text; the storage capacity of warez FTP servers is typically much greater.

35. Due to the volume of data at issue and the technical requirements set forth above, it may be necessary that the above-referenced equipment, software, data, and related instructions be seized and subsequently processed by a qualified computer specialist in a laboratory setting. Under the appropriate circumstances, some types of computer equipment can be more readily analyzed and pertinent data seized on-site, thus eliminating the need for its removal from the premises. One factor used in determining whether to analyze a computer on-site or to remove it from the premises is whether the computer constitutes an instrumentality of an offense and is thus subject to immediate seizure as such -- or whether it serves as a mere repository for evidence of a criminal offense. Another determining factor is whether, as a repository for evidence, a particular device can be more readily, quickly, and thus less intrusively, analyzed off-site, with due considerations given to preserving the integrity of the evidence. This, in turn, is often dependent upon the amount of data and number of discrete files or file areas that must be analyzed, and this is frequently dependent upon the particular type of computer hardware involved. As a result, it is ordinarily impossible to appropriately analyze such material without removing it from the location where it is seized.

36. Based upon my knowledge, training, and experience, as well as information related to me by agents and others involved in forensic examination of computers, I am aware that searches and seizures of evidence from computers taken from the premises commonly require agents to seize most or all of a computer system's input/output and peripheral devices, in order for a qualified computer expert to accurately retrieve the system's data in a laboratory or other controlled environment. Therefore, in those instances where computers are removed from the premises, in order to fully

retrieve data from a computer system, investigators must seize all the storage devices, as well as the central processing units (CPUs), and applicable keyboards and monitors which are an integral part of the processing unit. If, after inspecting the input/output devices, system software, and pertinent computer-related documentation, it becomes apparent that these items are no longer necessary to retrieve and preserve the data evidence, and are not otherwise seizable, such materials and/or equipment will be returned within a reasonable time.

Analysis of Electronic Data

37. The analysis of electronically stored data, whether performed on-site or in a laboratory or other controlled environment, may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, surveying various file directories and the individual files that they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer capable of containing pertinent files, in order to locate the evidence authorized for seizure by the warrant); examining all the structured, unstructured, deleted, and overwritten data on a particular piece of media; opening or reading the first few pages of such files in order to determine their precise contents; scanning storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic key-word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

Conclusion

38. Based on the information outlined above, the undersigned submits that there is probable cause to believe that the items identified in Attachment A have been used in the commission of a

crime and constitute evidence, contraband, fruits, or instrumentalities of violations of Title 17, United States Code, Section 506(a), and Title 18, United States Code, Sections 371 and 2319, and will be found at the premises to be searched.

Special Agent Walter J. Steffens, Jr.
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence this 20 day of April, 2004.

THE HONORABLE MARY PAT THYNGE
UNITED STATES MAGISTRATE JUDGE
DISTRICT OF DELAWARE

AO 93 (Rev. 5/85) Search Warrant

United States District Court

DISTRICT OF DELAWARE

In the Matter of the Search of
(Name, address or brief description of person or property to be searched)
[redacted]
Rehoboth Beach, Delaware, described more particularly on Attachment 1

SEARCH WARRANT

CASE NUMBER: 04-

TO: Special Agent Walter J. Steffens, Jr. and any Authorized Officer of the United States

Affidavit(s) having been made before me by Special Agent Walter J. Steffens, Jr. (Affiant) who has reason to believe that ☐ on the person of or ☒ on the premises known as (name, description and/or location)

[redacted] Rehoboth Beach, Delaware, described more particularly on Attachment 1

in the _____ District of Delaware there is now concealed a certain person or property, namely (describe the person or property)

items described on Attachment A

I am satisfied that the affidavit(s) and any recorded testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this warrant.

YOU ARE HEREBY COMMANDED to search on or before _____ (Date)

(not to exceed 10 days) the person or place named above for the person or property specified, serving this warrant and making the search (in the daytime — 6:00 A.M. to 10:00 P.M.) (at any time in the day or night as I find reasonable cause has been established) and if the person or property be found there to seize same, leaving a copy of this warrant and receipt for the person or property taken, and prepare a written inventory of the person or property seized and promptly return this warrant to _____ (U.S. Judge or Magistrate) as required by law. You are further authorized to comply with the conditions set forth in Attachment B.

_____ at Wilmington, Delaware
Date and Time Issued — City and State

Honorable Mary Pat Thynge
United States Magistrate Judge
Name and Title of Judicial Officer

_____
Signature of Judicial Officer

Attachment 1

[redacted] Rehoboth Beach, Delaware. [redacted] is a taupe bungalow with white trim and black shutters. The front door is black with a brass kick plate. A garage (taupe with a white door) is attached to the house. A mailbox is mounted on a white post set at the curb in front of the house. The numbe[redacted]e mounted vertically on the mailbox post.

Attachment A: Items to be seized

Items evidencing violations of Title 17, United States Code, Section 506(a), and Title 18, United States Code, Sections 371 and 2319(a), including but not limited to the following:

1. Computer files protected by copyright, including but not limited to software, game, movie and music titles.

2. Computer log files relating to copyright infringement, including but not limited to transfer logs of FTP uploads and downloads.

3. Computer files containing communications between individuals relating to copyright infringement, including but not limited to IRC and instant messaging logs, and emails.

4. Programs or software used by those engaging in copyright infringement, such as burning tool programs and software used for FTP file transfers (e.g. FlashFXP).

5. Records, in whatever form, of user names and passwords to "warez" sites and secure communication services.

6. Computer hardware, meaning any and all computer equipment. Included within the definition of computer hardware is any electronic device capable of data processing (such as central processing units, laptop or notebook computers, personal digital assistants, and wireless communication devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media); related communications devices (such as modems, cables and connections); storage media, defined below; and security devices, also defined below.

7. Computer software, meaning any and all data, information, instructions, programs, or program codes, stored in the form of electronic, magnetic, optical, or other media, which is capable of being interpreted by a computer or its related components. Computer software may also include data, data fragments, or control characters integral to the operation of computer software, such as operating systems software, applications software, utility programs, compilers, interpreters, communications software, and other programming used or intended to be used to communicate with computer components.

8. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

9. Data security devices, meaning any devices, programs, or data -- whether themselves in the nature of hardware or software -- that can be used or are designed to be used to restrict access to, or to facilitate concealment of, any computer hardware, computer software, computer-related documentation, or electronic data records. Such items include, but are not limited to, user names and passwords; data security hardware (such as encryption devices, chips, and circuit boards); data security software or information (such as test keys and encryption codes); and similar information

that is required to access computer programs or data or to otherwise render programs or data into usable form.

10. Records, in whatever form, referencing or regarding warez activity, warez sites, or individuals who participate in warez activity.

11. Storage media capable of collecting, storing, maintaining, retrieving, concealing, transmitting, and backing up electronic data used to conduct warez activity or which contains material or data obtained through warez activity. Included within this paragraph is any information stored in the form of electronic, magnetic, optical, or other coding on computer media or on media capable of being read by a computer or computer-related equipment, such as fixed hard disks, external hard disks, removable hard disks, floppy diskettes, compact disks (CDs), digital video disks (DVDs), tapes, optical storage devices, laser disks, or other memory storage devices.

12. Records, in whatever form, of personal and business activities relating to the operation and ownership of the computer systems, such as telephone records, notes, books, diaries, and reference materials.

13. Records, in whatever form, pertaining to accounts held with Internet Service Providers or of Internet use.

14. Evidence or records, in whatever form, relating to the ownership, occupancy, or use of the premises to be searched.

ATTACHMENT B

With respect to any computer hardware, computer software and computer storage media, authorization is hereby granted for the FBI, and other law enforcement officers under their direction and control, to remove all such items from the premises in order for them to be searched off the premises for the items described in Attachment A.